

Exhibit 160

access control

The process of granting or denying specific requests to: 1) obtain and use information and related information processing services; and 2) enter specific physical facilities (e.g., federal buildings, military establishments, border crossing entrances).

Source(s):

[NIST SP 800-12 Rev. 1](#) under Access Control ([FIPS 201-2](#))

The process of granting or denying specific requests: 1) for obtaining and using information and related information processing services; and 2) to enter specific physical facilities (e.g., Federal buildings, military establishments, and border crossing entrances).

Source(s):

[CNSSI 4009-2015](#) ([FIPS 201-1](#) - Adapted)

The process of permitting or restricting access to applications at a granular level, such as per-user, per-group, and per-resources.

Source(s):

[NIST SP 800-113](#) under Access Control

Procedures and controls that limit or detect access to critical information resources. This can be accomplished through software, biometrics devices, or physical access to a controlled space.

Source(s):

[NIST SP 800-192](#) under Access Control

[NISTIR 7316](#) under Access Control

Enable authorized use of a resource while preventing unauthorized use or use in an unauthorized manner.

Source(s):

[NIST SP 800-33](#)

[NIST SP 800-27 Rev. A](#) [Withdrawn]

Process of granting access to information system resources only to authorized users, programs, processes, or other systems.

Source(s):

[NIST SP 800-32](#) under Access Control

The process of granting access to information technology (IT) system resources only to authorized users, programs, processes, or other systems.

Source(s):

[NIST SP 800-47](#) under Access Control

Restricts resource access to only privileged entities.

Source(s):

[NIST SP 800-57 Part 1 Rev. 4](#) under Access control

Restricts access to resources only to privileged entities.

Source(s):

[NIST SP 800-57 Part 2](#) under Access control

The process of granting or denying specific requests to: (i) obtain and use information and related information processing services; and (ii) enter specific physical facilities (e.g., Federal buildings, military establishments, and border-crossing entrances).

Source(s):

[NIST SP 800-79-2](#) under Access Control

As used in this Recommendation, the set of procedures and/or processes that only allow access to information in accordance with pre-established policies and rules.

Source(s):

[NIST SP 800-57 Part 2 Rev.1](#) under Access control

The process of limiting access to resources of a system only to authorized programs, processes, or other systems (in a network).

Source(s):

[NISTIR 4734](#) under Access Control

To ensure that an entity can only access protected resources if they have the appropriate permissions based on the predefined access control policies.

Source(s):

[NISTIR 7497](#) under Access Control

The process of granting or denying specific requests for obtaining and using information and related information processing services.

Source(s):

[NISTIR 7711](#) under Access Control

The process of granting or denying specific requests: 1) obtain and use information and related information processing services; and 2) enter specific physical facilities (e.g., Federal buildings, military establishments, border crossing entrances).

Source(s):

[FIPS 201](#) under Access Control [version unknown]

Restricts access to resources to only privileged entities.

Source(s):

[NIST SP 800-57 Part 1 Rev. 3](#) under Access control [Superseded]